Cyberattacchi: l'Italia è maglia nera mondiale

Secondo i dati di Rubrik, oltre il 91% dei responsabili IT e della sicurezza italiani ammette di aver subito attacchi informatici lo scorso anno. Tra questi, il 96% delle aziende colpite ha pagato un riscatto a seguito di un attacco ransomware andato a buon fine.

Milano, 21 maggio 2025 - Una nuova ricerca dei Rubrik (NYSE: RBRK) Zero Labs conferma come le aziende si trovino ad affrontare un'ondata sempre più forte di attacchi informatici. Il 91% dei responsabili IT e della sicurezza italiani ha segnalato di aver subito cyber attacchi nell'ultimo anno, un dato leggermente superiore alla media globale del 90%. Il rapporto, intitolato "La sicurezza dei dati nel 2025: una crisi distribuita", mette in evidenza i rischi creati dagli ambienti ibridi, che stanno portando in particolare a una crisi della sicurezza cloud per la quale le organizzazioni non sono preparate.

"Molte aziende che migrano su ambienti cloud sono erroneamente convinte che sarà compito dei fornitori scelti occuparsi della sicurezza", ha affermato Joe Hladik, Head of Rubrik Zero Labs. "La persistenza degli attacchi ransomware, unita allo sfruttamento delle vulnerabilità del cloud ibrido, dimostra invece che gli autori delle minacce sono sempre un passo avanti. Le aziende devono agire e adottare una mentalità da attaccante, identificando - e proteggendo - i dati più preziosi, prima che sia troppo tardi. Dotarsi di una strategia di sicurezza incentrata sui dati che dia priorità alla visibilità, al controllo e al ripristino rapido non è mai stata così decisivo."

La frequenza e l'impatto dei cyberattacchi aumentano

I cyberattacchi sono una minaccia costante, come evidenziano diversi aspetti della ricerca:

- Quasi un quinto delle organizzazioni a livello globale ha subito più di 25 attacchi informatici solo nel 2024, secondo i responsabili IT e della sicurezza - la media è superiore a una violazione ogni due settimane.
- Violazioni dei dati (30%), malware sui dispositivi (29%), violazioni del cloud o del SaaS (28%), phishing (28%) e minacce interne (28%) sono state indicate come le tipologie di attacco più comuni a livello globale. I dati italiani parlano invece di violazioni di dati (37%), phishing (35%), minacce interne (34%) e interruzione della produzione da parte di insider o eventi non dolosi (34%).
- A livello globale, queste le principali conseguenze degli attacchi:
    - il 40% degli intervistati ha segnalato un aumento dei costi della sicurezza;
    - il 37% ha rilevato danni alla reputazione e perdita di fiducia dei clienti;
    - il 33% ha subito un cambio forzato di leadership a seguito di un incidente informatico;
    - per l'Italia la conseguenza maggiore è rappresentata dalle "perdite finanziarie" con il 41%, la percentuale più alta tra tutti i paesi intervistati.

Intelligenza artificiale, adozione del cloud e complessità dei dati creano nuove sfide

Proteggere i dati sensibili su più sistemi è diventata una sfida sempre più complessa, poiché l'adozione diffusa dell'AI ha amplificato in modo significativo la dispersione dei dati. Il 90% degli intervistati riferisce di gestire ambienti cloud ibridi e la metà dei responsabili IT afferma che la maggior parte dei carichi di lavoro è ora basata sul cloud.

La ricerca ha evidenziato inoltre che:

- Il 35% degli intervistati cita la sicurezza dei dati in questi diversi ecosistemi come la sfida principale da affrontare, seguita dalla mancanza di una gestione centralizzata (30%) e dalla scarsa visibilità e controllo sui dati basati sul cloud (29%). La preoccupazione principale indicata in Italia è la scarsa disponibilità di risorse per le operazioni di sicurezza (39%), la più alta tra i paesi intervistati.
- Il 36% dei file sensibili nel cloud è classificato come ad alto rischio ed è composto in gran parte da informazioni di identificazione personale (PII), come numeri di previdenza sociale e numeri di telefono; seguono dati digitali e dati aziendali, come proprietà intellettuale e codice sorgente (Dati telemetrici di Rubrik).

Ransomware e minacce all'identità si evolvono di pari passo

Il ransomware rimane una minaccia persistente e in continua evoluzione:

- Tra le organizzazioni che hanno subito un attacco ransomware di successo lo scorso anno, l'86% ha ammesso di aver pagato un riscatto per recuperare i propri dati. In Italia questo è un fenomeno ancor più diffuso, con dati che raggiungono il 96%.
- Quasi tre quarti (74%) hanno ammesso che i loro sistemi di backup e ripristino sono stati parzialmente compromessi dagli attori delle minacce, il 35% addirittura ha affermato che i loro sistemi sono stati completamente compromessi. In Italia, il dato è più favorevole, con il 58% dei dati di backup che sono stati, anche solo parzialmente, compromessi e il 24% totalmente compromessi.

Le minacce all'identità si stanno intensificando, alimentate dalla complessità degli ambienti ibridi di oggi:

- Con il 92% (93% in Italia) delle organizzazioni che utilizzano da due a cinque piattaforme cloud e SaaS, gli attaccanti sfruttano i punti deboli nella gestione delle identità e degli accessi per muoversi lateralmente e intensificare gli attacchi ransomware.
- Il 28% dei responsabili IT ha citato le minacce insider, spesso causate da credenziali compromesse, sottolineando la crescente difficoltà di mantenere forti controlli sugli accessi nei sistemi distribuiti. In Italia questo dato sale al 34%.
- La telemetria di Rubrik rivela che il 27% dei file sensibili ad alto rischio contiene dati digitali come chiavi API, nomi utente e numeri di account: esattamente il tipo di informazioni che gli hacker cercano per dirottare le identità e infiltrarsi nei sistemi critici.

Per leggere il report completo, visitare il sito https://zerolabs.rubrik.com/

Metodologia

"La sicurezza dei dati nel 2025: una crisi distribuita" si basa su dati raccolti da oltre 1.600 leader IT e della sicurezza in 10 Paesi (metà dei quali erano CIO o CISO), nel corso di una ricerca condotta in collaborazione con Wakefield. I risultati sono arricchiti dai dati telemetrici di Rubrik, tra cui l'analisi di 5,8 miliardi di file totali in ambienti cloud e SaaS, con oltre 175 milioni di file sensibili classificati negli ambienti dei clienti. I dati fanno riferimento al periodo tra il 1° gennaio e il 31 dicembre 2024.

Rubrik

Rubrik (NYSE: RBRK) è in missione per proteggere i dati del mondo. Con la Zero Trust Data Security™, aiutiamo le organizzazioni a raggiungere la resilienza aziendale contro i cyberattacchi, gli insider malintenzionati e le interruzioni operative. Rubrik Security Cloud, basato sul machine learning, protegge i dati nelle applicazioni aziendali, cloud e SaaS. Aiutiamo le organizzazioni a mantenere l'integrità dei dati, a garantire una disponibilità dei dati che resista a

condizioni avverse, a monitorare costantemente i rischi e le minacce ai dati e a ripristinare le aziende con i loro dati quando l'infrastruttura viene attaccata. Per maggiori informazioni visitate il sito www.rubrik.com e seguite @rubrikInc su X (conosciuto precedentemente come Twitter) e Rubrik su LinkedIn.

Ufficio stampa:
Axicom Italy
rubrikitaly@axicom.com